Interview Summary

Initially, Applicants wish to thank Examiner Hoang and Supervisor Moazzami for the courtesies extended to Applicants' representative during the telephonic interview of October 29, 2009. The parties discussed the rejections of claims 1-22, 25, 27-34, 36, 40-41 and 43-46 under 35 U.S.C. § 103(a) over Khidekel (U.S. Patent App. Pub. No. 2001-0027527, hereinafter "Khidekel") in view of Ballantyne (U.S. Patent No. 5,867,821, hereinafter "Ballantyne"). Agreement was reached that Khidekel did not disclose, at least, "recording each access operation[,]" as recited, for example, in claim 1. No agreement was reached with respect to Ballantyne. The Examiner stated that should the present application be appealed, prosecution would likely be reopened and Ballantyne asserted as a primary reference. The present Request for Reconsideration is filed considering the Examiner's comments.

REMARKS

Reconsideration of the present application in light of the following remarks is respectfully requested.

Claims 1-22, 25, 27-34, 36, 40, 41 and 43-46 are pending. Claims 1, 9, 29 and 40 are in independent form.

REJECTION UNDER 35 U.S.C. § 103 – *KHIDEKEL/BALLANTYNE*

Claims 1-22, 25, 27-34, 36, 4, 41 and 43-46 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Khidekel in view of Ballantyne. Applicants respectfully traverse these rejections.

Claim 1 recites, *inter alia*, "performing a security check upon each access operation in order to ascertain the identity of a user; assigning a user signature, identifying the user, on the basis of the performed security check without being viewable by the user ... assigning at least one role signature, each role signature being assignable to a plurality of users, on the basis of the performed security check without being viewable by the user ... signing each access operation to electronic data by specifying the user signature and the at least one role signature; and recording each access operation and the user signature and the at least one role signature specified for each access operation[.]"

Khidekel does not disclose, at least, a "signature[,]" as recited by claim 1. Khidekel only discloses techniques for allowing or denying access requests or transactions.

Khidekel discloses authenticating a user based on the user's credentials (Khidekel, ¶. [0029]) or based on digital certificates (Khidekel, ¶. [0030]). Khidekel authenticates the user's credential and stores a time stamped record of the authentication. Khidekel, ¶. [0033]. A secured server is then sent a token based on information such as the user's credentials. If a user attempts to gain access to records, a secure server validates the token by comparing "the difference between the current time and the authentication time to a predefined threshold. For example, a hospital might define the threshold as one month." Khidekel, ¶. [0035]. Khidekel nowhere discloses a user signature or a role signature.

Although the Office Action attempts to equate the user's signature to a "token" (Office Action p. 2), Applicants note that claim 1 recites, *inter alia*, "performing a security check upon each access operation in order to ascertain the identity of a user; assigning a user signature, identifying the user, on the basis of the performed security check without being viewable by the user[.]" Applicants note that Khidekel performs a security check using the issued token and the issued token is not assigned based on the security check. Khidekel, ¶¶. [0036].

Further, the Office Action attempts to equate a "role signature[,]" as recited by claim 1 with "business rules that indicate which users are authorized to take various types of action[.]" Office Action, p. 3. However, business rules are not assigned, "on the basis of the performed security check without being viewable by the user[,]" and therefore cannot be a "role signature[,]" as recited by claim 1.

Ballantyne also does not disclose, at least, a "signature[,]" as recited by claim 1. Ballantyne discloses a, "security process ... based on the identification and authentication of individuals requesting access to the health records of the database." Ballantyne, col. 7, l. 66 through col. 8, l. 2. A user may be assigned a unique identification number (ID). Ballantyne, col. 8, ll. 20-22. However, the ID is used as part of a security check and is not assigned "on the basis of the performed security check[,]" as recited by claim 1. Further, the ID is not assigned, "without being viewable by the user[,]" as recited by claim 1.

Ballantyne discloses that in order to gain access, a user "enters their ID number[.]" Ballantyne, col. 8, l. 29.

The Office Action attempts to equate, "the personal electronic profile" of Ballantyne with the "role signature" of claim 1. However, the only information stored in the personal electronic profile, as specifically disclosed by Ballantyne, is the user's "mother's name[.]" Ballantyne, col. 8, ll. 34-36. Ballantyne nowehere discloses that the user profile is "assignable to a plurality of users[,]" as recited by claim 1. Ballantyne discloses that a user profile is "personal[.]"

Even assuming, *arguendo*, that Khidekel does disclose a signature (which Applicants disagree with), Khidekel nowhere discloses, "signing each access operation to electronic data by specifying the user signature and the at least one role signature; and recording each access operation and the user signature and the at least one role signature specified for each access operation[,]" as recited by claim 1, emphasis added. Khidekel only discloses that, "[t]he authentication server 12 authenticates the user's credentials and stores 66 **a time-stamped record of the authentication**. Khidekel, ¶. [0033]. As may be appreciated, a time-stamped record of an authentication is different than recording each access operation, a user signature and a role signature, each access operation. Further, Khidekel specifically notes that, "[u]se of the threshold can eliminate the need for the user to authenticate with the server 12 each time he wishes to access information on the secure server 36." Khidekel, ¶. [0036]. For this reason, authentication does not occur every access operation according to Ballantyne.

The Office Action attempts to equate the recording of each access operation of claim 1 with a secure server's validation of a token, stating that, "if each access operation is not logged, there would be an error in the duration of time since the last access operation that was not logged." Office Action, p. 2. However, Khidekel only compares the current access operation with a time stamp of the most recent **authentication**, which is stored in the token. Khidekel, ¶. [0035]. For this reason, the time of a previous access operation is not relevant and Khidekel need not inherently record each access operation as alleged.

Further, the Office action relies on the alleged inherent necessity of recording the last access operation to show recordation of a user signature and a role signature each access operation. Office Action, p. 3. Accordingly, the Office Action also fails to show that recordation of a user and role signature occurs each access operation.

Ballantyne also does not disclose, at least, "signing each access operation to electronic data by specifying the user signature and the at least one role signature; and recording each access operation and the user signature and the at least one role signature specified for each access operation[,]" as recited by claim 1, emphasis added. Ballantyne discloses, "[a]ll authorized users that access any patient record, their name and time of access are all documented[.]" Ballantyne, col. 8, ll. 54-56. As noted above, Ballantyne does not disclose a signature as recited by claim 1. However, even assuming that the user's name may be interpreted as a user signature within the meaning of claim 1 (which

Applicants disagree with for at least the reasons stated above), Ballantyne does not disclose recording each access operation with at least one role signature, "each role signature being assignable to a plurality of users[,]" as recited by claim 1. Applicants note that Ballantyne may disclose roles (e.g., classifications) for use in access restrictions (e.g., Ballantyne col. 8, ll. 7-10 and col. 10, ll. 10-15). However, Ballantyne nowhere discloses a role signature or, "recording .. the at least one role signature specified for each access operation[,]" as recited by claim 1.

Further, the Office Action attempts to equate the user ID of Ballantyne with the user signature of claim 1, and the user profile of Ballantyne with the role signature of claim 1. However, Ballantyne nowhere discloses recording the user profiles or the ID each access operation.

Applicants note for explanatory purposes that according to claim 1, a user signature and a role signature is recorded for each access operation. Accordingly, an audit may be performed to determine not only who participated in the access operation, but also in which role they performed the access operation. This is not possible according to either Khidekel or Ballantyne.

Therefore, even assuming, arguendo, that Khidekel and Ballantyne could be combined (which Applicants do not admit), at least because neither Khidekel nor Ballantyne, alone or in combination, disclose every element of claim 1, Khidekel in view of Ballantyne cannot render claim 1 obvious. Claims 9, 29 and 40 are patentable for reasons at least similar to those stated above with respect to claim 1, noting that claims 9, 29 and 40 should be interpreted solely

based on the limitations recited therein. Claims 2-8, 10-22, 25, 27, 28, 30-34, 36, 41 and 43-46 are patentable at least by virtue of their dependence on at least one of claims 1, 9, 29 or 40. Withdrawal of the rejections and allowance of each of claims 1-22, 25, 27-34, 36, 40, 41 and 43-46 is respectfully requested.

CONCLUSION

Accordingly, in view of the above amendments and remarks, reconsideration of the objections and rejections and allowance of each of the pending claims in connection with the present application is earnestly solicited.

Should there be any outstanding matters that need to be resolved in the present application, the Examiner is respectfully requested to contact Donald J. Daley at the telephone number of the undersigned below.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 08-0750 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. §1.17; particularly, extension of time fees.

Respectfully submitted,
HARNESS, DICKEY, & PIERCE, P.L.C.

By _____, 41,018
Donald J. Daley, Reg. No. 34,313

DJD/AXV

P.O. Box 8910
Reston, Virginia 20195
(703) 668-8000
John Fitzpatrick